RSA SecurID Ready Implementation Guide

Last Modified: January 7, 2008

Partner Information

Product Information	
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	Cisco VPN Client
Version & Platform	4.6, 4.8, and 5.0.02.0090
Product Description	Simple to deploy and operate, the Cisco VPN Client allows organizations to establish end-to-end, encrypted VPN tunnels for secure connectivity for mobile employees or teleworkers. This thin design, IP security (IPSec)-implementation is compatible with all Cisco virtual private network (VPN) products.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)

Solution Summary

The Cisco VPN Client allows users to RSA SecurID Authenticate to establish end-to-end, encrypted VPN tunnels for secure connectivity for mobile employees or teleworkers. This authentication can be done with either Native RSA SecurID authentication or with RADIUS. The end user running on a Windows platform can also take advantage of additional integration work by using the RSA Software Token or the RSA SecurID 800 token. The Cisco VPN client can pull the tokencode from the RSA Software Token or RSA SecurID 800 token running on the same machine and couple the PIN and tokencode so that users only need to enter their PIN during an authentication.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication and RADIUS
RSA Authentication Manager Name Locking	Server Dependant
RSA Authentication Manager Replica Support	Yes (Authentication Manager v6.x and above)
RSA Software Token and RSA SecurID 800 Automation	Yes
Use of Cached Domain Credentials	No

Product Requirements

Partner Product Requirements: Cisco VPN Client	
Memory	34 MB
Storage	50 MB

Operating System	
Platform	**Required Patches**
Windows XP	SP2 or later
Windows 2000	SP2 or later
Windows Vista	All versions as of date listed above

Additional Hardware Requirements:

The Cisco VPN Client is compatible with the following Cisco products

- Cisco VPN 3000 Series Concentrator Software Version 3.0 or later
- Cisco IOS Software Release 12.2(8)T or later
- Cisco PIX Security Appliance Software Version 7.0 or later
- Cisco ASA 5500 Series Software Version 7.0 or later

The Cisco VPN Client integrates with the RSA Software Token and RSA SecurID 800 token so that users only have to enter a PIN; where the tokencode is automatically pulled into the client. The following table shows what Cisco products support this feature.

RSA Software Token and RSA SecurID 800 Integration Compatibility Matrix		
Cisco Product	**Native RSA SecurID Authentication**	**RADIUS Authentication**
Cisco VPN 3000 Series	Yes	Yes*
Cisco IOS Software	N/A	No
Cisco PIX Security Appliance	Yes	Yes*
Cisco ASA 5500 Series	Yes	Yes*
	* Needs RadiusSDI set to 1 for this to function. See the Cisco VPN client profile configuration section for information.	

Important: The RSA Software Token and RSA SecurID 800 Integration is a Windows only solution.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

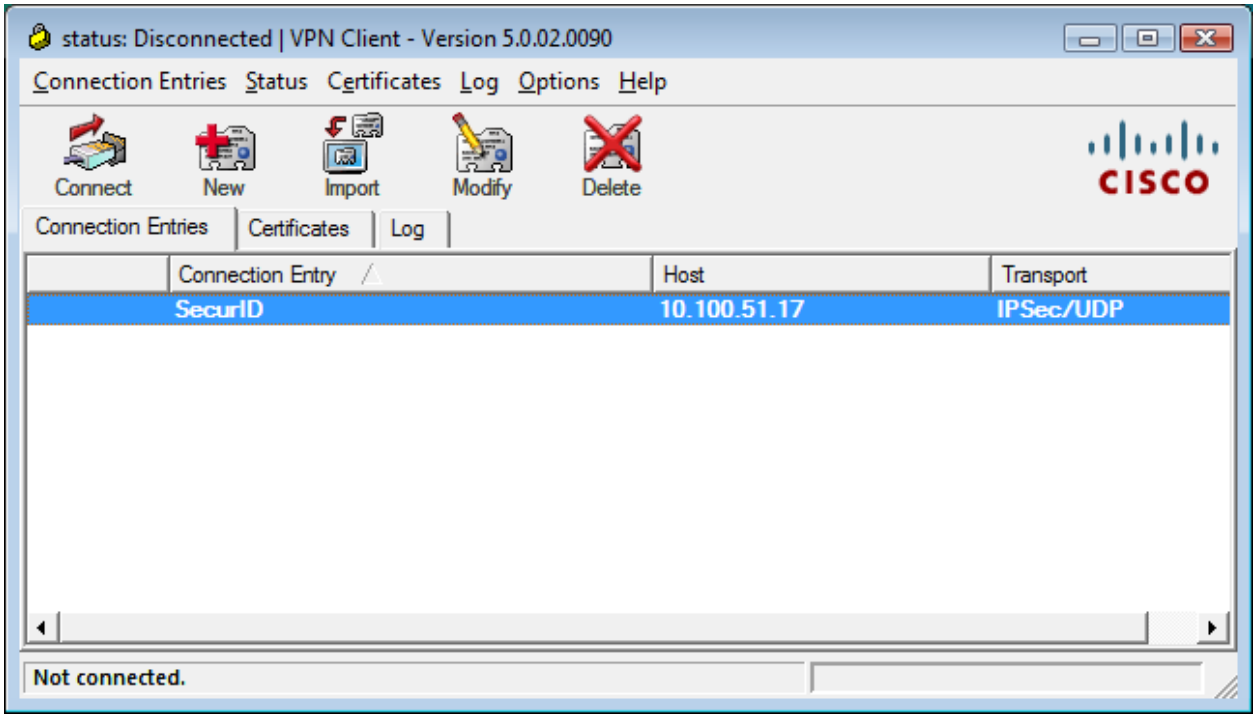
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

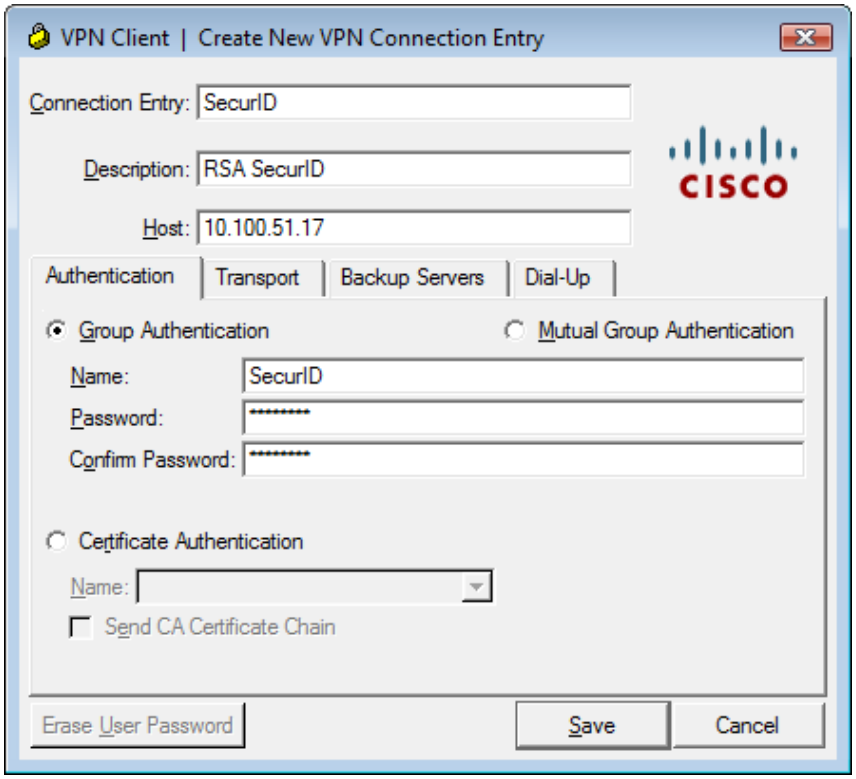
Documenting the Solution

Cisco VPN Client Configuration

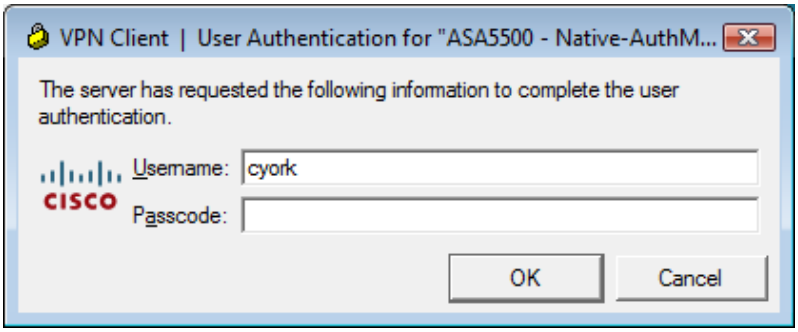
1. Install the Cisco VPN client and then start the application.



2. Click the **New** button to create an RSA SecurID connection entry. Fill in the appropriate information for the connection. The group name and password must match the entry you create on the VPN server device.



3. Click Save.
4. Highlight the connection created and click connect.
5. The user will be prompted for authentication information.



RSA Software Token and RSA SecurID 800 Integration:

RSA Software Token and RSA SecurID 800 Token integration with the Cisco VPN client is dependent on the Cisco VPN server. See the comparability matrix under the Product Requirements section for more details. If the Cisco VPN client detects that the RSA Software Token or RSA SecurID 800 Token is installed (through the presence of stauto32.dll), users will be prompted for their PIN only. The tokencode displayed on the RSA Software Token or RSA SecurID 800 Token is automatically coupled with the PIN and passed along to the RSA Authentication Manager. You can turn on and off the option for the PIN only prompt when using the Cisco VPN client 4.x. See the Cisco VPN client profile configuration parameters section for more information.

Cisco VPN client profile configuration parameters:

You can enable and disable the ability of the Cisco VPN client to only prompt the user for their PIN when using the RSA Software Token or the RSA SecurID 800 Token by adding the following setting in your profile file. This file is located by default in Program Files\Cisco Systems\VPN Client\Profiles. The file name is the name of the connection entry with a .pcf extension.

SDIUseHardwareToken = 0 or 1

0 = Yes use RSA Software Token (default)

1 = No, ignore RSA Software Token installed on the PC.

You can also change the prompts displayed to a user that is authenticating using RADIUS to better resemble an RSA SecurID authentication by setting the following parameter in the profile file.

> **Note: This setting will also allow the RSA Software Token and RSA SecurID 800 automation to work when using RADIUS as the authentication method with some Cisco VPN servers. See the comparability matrix under the Product Requirements section of this guide along with the Cisco documentation for more details.**

RadiusSDI

0 = No (default)

1 = Yes

See the Cisco VPN client documentation for more information on these and other settings that can be used.

Certification Checklist

See the RSA Security Implementation guide for each Cisco VPN server device for certification testing information.

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_VPN3K_47_AuthMan61.pdf

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_Router_VPN_12_4_AuthMan61.pdf

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_PIX_702_AuthMan61.pdf

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_ASA_AuthMan61.pdf